UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,026	09/21/2000	William T. Jennings	064751.0298	8477

45507	7590	05/04/2005		EXAMINER	

BAKER BOTTS LLP
2001 ROSS AVENUE
6TH FLOOR
DALLAS, TX 75201

EXAMINER
LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)	
Office Action Summary	09/668,026	JENNINGS, WILLIAM T.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *01 July 2004*.

2a) ☒ This action is **FINAL.**   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-36* is/are pending in the application.

    4a) Of the above claim(s) *25* is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-24 and 26-36* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some *   c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *7/26/04*.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   The amendment of 01 July 2004 has been noted and made of record.

2.   Claims 1-36 have been presented for examination.

3.   Claim 25 has been cancelled as per Applicant's request.

Response to Arguments

4.   In response to the Applicant's argument that Merkle does not disclose randomly selecting
at the receiver one of the trap door encryption function pairs and the corresponding token, the
Examiner disagrees. Merkle discloses on page 296, column 2, that Y (who receives the puzzle
and ID from X) selects a puzzle at random, and then transmits the ID back to X over the key
channel. Therefore, Merkle does disclose randomly selecting at the receiver one of the trap door
encryption function pairs and the corresponding token.

5.   In response to applicant's argument that the examiner's conclusion of obviousness is
based upon improper hindsight reasoning, it must be recognized that any judgment on
obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so
long as it takes into account only knowledge which was within the level of ordinary skill at the
time the claimed invention was made, and does not include knowledge gleaned only from the
applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392,
170 USPQ 209 (CCPA 1971).

6.   Applicant's arguments with respect to claims 1-24 and 26-36 have been considered but
are moot in view of the new ground(s) of rejection.

7.   See further rejections that follow.

Claim Rejections - 35 USC § 103

8.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

9.   Claims 1-3, 6-8, 10-12, 14-20, 22-24, 26-30, and 32-36 are rejected under 35 U.S.C.

103(a) as being unpatentable over "Secure Communications Over Insecure Channels," by Ralph

C. Merkle, hereinafter Merkle, in view of U.S. Patent No. 5,481,613 to Ford et al, hereinafter

Ford.

10.   As per claims 1, 6, 14, 28, and 33, Merkle teaches creating a set of N trap door

encryption-decryption function pairs each paired with a corresponding token; transmitting the set

of N trap door encryption-decryption function pairs along with a corresponding token to a

receiver', randomly selecting at the receiver one of the trap door encryption-decryption function

pairs and the corresponding token; recording in a key escrow database the created set of N trap

door encryption decryption function pairs and the corresponding paired token; recording in the

key escrow database the randomly selected trap door encryption decryption function pair along

with the encrypted token; and inverting the created set of N trap door encryption-decryption

function pairs and the randomly selected trap door encryption-decryption function pair along

with the encrypted token to identify the decryption key (pages 296-299).

11.   Merkle does not disclose adding randomization information at the receiver to the

corresponding token of the selected trap door encryption-decryption function pair and encrypting

the token with the added randomization information, the token corresponding with the randomly

selected encryption-decryption function pair.

12.   Ford teaches returning the identifier back to the key release agent in a locally protected transaction (column 4, lines 24-29; column 4, lines 50-54).

13.   It would have been obvious to one of ordinary skill in the ad at the time the invention was made to add randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypt the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair, as apposed to sending it back unencrypted as Merkle suggests, since Ford discloses at column 3, line 62 to column 4, line 12 that such a modification would allow secure distribution of an encryption key to client who are authorized according to a set of access control attributes, provide a method of recovering an encryption key from a key release agent in a secure manner, provide a method of recovering an encryption key from an encrypted access controlled decryption block which contain access control attributes, and provide a key release agent releasing an encryption key to a party other than a client that is explicitly authorized.

14.   As per claims 2 and 29, Merkle teaches encrypting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door function along with the decryption key prior to recording in the key escrow database (page 298).

15.   As per claims 3, 7, 14, 30 and 36, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n^2)$. Having the receiver choose more than one puzzles slightly

increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations.

16.   As per claim 8, Merkle teaches decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information (page 299).

17.   As per claim 10, Merkle teaches the utilization of a symmetrical cryptosystem (page 296).

18.   As per claim 11, Merkle teaches the utilization of a public key cryptosystem (page 299).

19.   As per claims 12 and 35, Merkle teaches wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs and a response message from the receiver prior to recording (page 296).

20.   As per claim 15, Merkle teaches decrypting at the receiver the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair (page 296).

21.   As per claims 16 and 32, Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram comprising', the corresponding token, the decryption key and randomization information (page 298).

22.   As per claim 17, Merkle teaches decoding the encrypted escrow key comprises selecting

a decryption key randomly from a selected group of decryption keys (page 296).

23.   As per claim 18, Merkle teaches comprising recognizing a correct decoding result

utilizing structural information embedded in the response message (page 296).

24.   As per claim 19, Merkle teaches creating at an originator further comprises generating the

set of N trap door functions utilizing a selected encryption function and a private encryption key

(page 297).

25.   As per claims 24 and 34, Merkle does not explicitly teach the receiver selecting more

than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in

the art would know that the work needed to be performed by an eavesdropper plotting to learn

the decryption key is $O(n^2)$. Having the receiver choose more than one puzzles slightly increases

the poor security of Merkle's system by forcing the eavesdropper to perform more calculations.

Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram

comprising', the corresponding token, the decryption key and randomization information (page

298).

26.   As per claim 23 and 25, Merkle teaches the utilization of a symmetrical cryptosystem

(page 296).

27.   As per claim 24, Merkle teaches the utilization of a public key cryptosystem (page 299).

28.   As per claim 26, Merkle teaches recording in an escrow database the created N trap door

functions along with each corresponding token and the encrypted escrow key with the randomly

selected trap door function (page 298).

29.   As per claim 27, Merkle teaches inverting the recorded set of N trap door functions and

the encrypted escrow key with the randomly selected trap door function to identify a decryption

key from the key escrow database (page 297 and 298).

30.   Claims 4, 5, 9, 13, 21, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Merkle in view of Ford as applied above, and further in view of U.S. Patent No. 5,815,573

to Johnson et al., hereinafter Johnson.

31.   As per claims 4, 5, 31 Merkle teaches using identifying information to distinguish when

puzzles have been correctly solved (page 296).

32.   Merkle and Ford do teach the use of a digital signature. Merkle does teach that keys are

looked up based upon a user (page 298). Therefore there is a need to have a positively

identifying means to ascertain the correct author of a published key.

33.   Johnson teaches the use of a digital signature (column 10, lines 61-63). In view of this it

would have been obvious to one of ordinary skill in the art at the time of the invention to employ

the teachings of Johnson et al within the combined system of Merkle and Ford because it would

associate a key to a user with provable certainty.

34.   As per claim 9, Merkle and Ford do not teach explicitly using a linear transformation to

combine the token information.

35.   Johnson teaches the use of linear transformation to add keys together (figure 1, element

110). In view of this it would have been obvious to one of ordinary skill in the art at the time of

the invention to employ the teachings of Johnson within the combined system of Merkle and

Ford because linear transforms are a fast well established operation in order to carry out

transformations.

36.   As per claims 13 and 21, Merkle teaches using identifying information to distinguish

when puzzles have been correctly solved (page 296).

37.   Merkle and Ford do teach the use of a digital signature. Merkle does teach that keys are

looked up based upon a user (page 298). Therefore there is a need to have a positively

identifying means to ascertain the correct author of a published key.

38.   Johnson teaches the use of a digital signature (column 10, lines 61-63).

39.   In view of this it would have been obvious to one of ordinary skill in the art at the time of

the invention to employ the teachings of Johnson with the combined system of Merkle and Ford

because it would associate a key to a user with provable certainty.

Conclusion

40.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

41.   A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

42.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792.

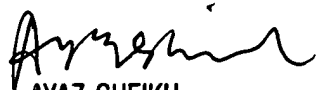The examiner can normally be reached on Monday thru Thursday 7-5.

43.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

44.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100